



Cellebrite

Digital intelligence
for a safer world

JFED Analytics Enterprise

Alameda County Sheriff Department

June 5, 2018



Contents

1. Introduction	5
2. Data analysis	7
2.1. Interactive filtering	7
2.2. Free text search	9
2.3. Faceted filters	9
2.4. Media analytics	11
2.4.1. Image and video categorization	11
2.4.2. Video category synopsis	12
2.5. Media similarity	12
2.5.1. Face Similarity Recognition	13
2.5.2. Image similarity recognition	13
2.6. Optical character recognition	14
2.7. Text analytics – Entity extraction	14
2.8. Language identification	16
2.9. Contextual views	17
2.9.1. List view	17
2.9.2. Graph view	18
2.9.3. Conversation view	18
2.9.4. Map view (Geolocation view)	19
2.9.5. Media view	20
2.10. Person view	20

2.11. Explore view -----	21
3. Data management -----	23
3.1. Data flow-----	23
3.2. Data intake process-----	23
3.3. Automated case creation -----	23
3.4. Automated decoding-----	24
3.5. Storage optimization -----	24
3.6. Supported data sources -----	25
3.7. Case management -----	26
3.8. User management -----	26
3.9. Security model-----	26
3.10. Cross-case analysis-----	27
3.11. User client and information sharing-----	27
3.12. Reports -----	28
3.12.1. Forensic reports -----	28
3.12.2. Investigative reports-----	29
3.12.3. Report history-----	30
3.13. WalkMe interactive onboarding -----	31
3.14. Basic UFED analytics server specifications-----	34
3.15. Project resources-----	35
3.16. Budgetary pricing-----	36

1. Introduction

Cellebrite's Analytics is designed to increase the impact of digital forensic data, empowering agencies to become more productive, efficient and successful – all while managing digital data.

Digital data has an important and almost existential place in peoples' everyday lives. Consequently, digital data is an important cornerstone of any investigation.

Due to the complexities inherent in analyzing digital data, most agencies are not truly benefiting from the full impact of the wealth of digital forensic data that was already collected – and is readily available.

While digital data will continue to be a forensic specialist field in the area of acquisition and extraction, Analytics provides data consumers with a tool for quicker and deeper analysis – where each event maintains a direct link to the evidence sources.

The key component of Analytics may be summarized in one word: accessibility.

Analytics enables you to:

- Simplify complex analysis tasks and make case resolution as easy as clicking a button.
- Share data among multiple agents to collaboratively accelerate investigations.
- Centrally manage your digital data to reduce risk and minimize storage requirements.

2. Data analysis

Digital forensic data is a challenging data source. Today, the common practice of using a report does not fully enable you to benefit from the huge impact that digital forensic data may have on any case in a timely manner, or even at all.

The Analytics data analysis module is based on three main sub-modules:

- **Interactive filtering:** Search and filter options allowing the user to select the data to be retrieved and analyzed.
- **Contextual views:** Different views allowing the user to display the selected data. Views include event lists, link analysis graphs, geographical presentations of locations on a map and a dedicated view for the analysis of multimedia.
- **Details view:** Zoom-in capability to analyze the details of a specific entity.

The following sections describe the highlights of these sub-modules.

2.1. Interactive filtering

The interactive filtering sub-module allows the user to apply filtering criterion, using a variety of data types to define the dataset retrieved from the database.

The following are the list of parameters that can be used as standalone components or combined with other parameters as filters in the system:

Parameter	Description
Cases	Determine the case or list of cases. Only events related to these cases will be retrieved.
Owners	Retrieve events related to specific device owners.
Extractions	Retrieve events from specific extractions.
Source	Retrieve events from a specific data source.
Timeframe	Retrieve events from a specific timeframe.
Hash databases	Retrieve events containing a match to specific, known hashes

Parameter	Description
Parties	Retrieve events in which the parties participated in (e.g. all personal correspondence with John Doe).
Identifiers	Retrieve events related to a specific phone number, email address, user name, etc.
Type	Retrieve events of a specific type (i.e. Call log, messages, pictures etc.).
Languages	Select events in a specific language.
Tags	Retrieve events with a specific tag. (While reviewing events, the investigator can apply a tag to flag these events for future reference. Each event can have multiple tags.)
Watch list	Retrieve events containing phrases on a specific watch list.
Entities	Retrieve events consisting of auto extracted entities (see more details below).
Media tags	Retrieve media categorized under a specific media category (see more details below).
System tags	Retrieve events categorized under a specific system tag.
Source	Retrieve events from a specific source application.
States	Retrieve events categorized by current state (intact, deleted or unknown).
File types	Retrieve specific file types. Certain file types are identified and tagged in the extracted data. There are eight default tags: Applications, Audio, Configurations, Databases, Documents, Images, Text, and Videos.
Priority	Retrieve email events categorized by priority.
Geodistance	Retrieve events occurring within specific geographical distance parameters.

Any filter can be locked so that it will not be cleared even if the Clear filter button is clicked.

2.2. Free text search

Cellebrite's unique processing technology for big data indexing and searching ensures that all the events, their metadata, automated analytics and categorization are all indexed and stored. The user does not need to burden themselves with selecting what and where to index.

This means that huge mounds of extractions become manageable, and users know where data sources are and what they contain – a virtual forensic library with rich details, querying capabilities and extremely responsive performance.

Search in a Google-like user experience for any value or sub value; results are culled from all content, files, attachments and metadata. Search the entire system – out of tens of millions¹ of events – to pinpoint the one event that you need. Benefit from a friendly auto-suggest feature to cue and focus on relevant pieces of information.



2.3. Faceted filters

Analytics offers a rich filtering mechanism that allows users to slice & dice the data using different parameters. Using faceted filtering is an efficient way to explore large amounts of data, displaying summaries about various dimensions of the data and allowing for the narrowing of the navigation down to a specific dimension value. This is achieved by maintaining multiple dimensions (facets) for each event and thus enabling events to be accessed and ordered in multiple ways.

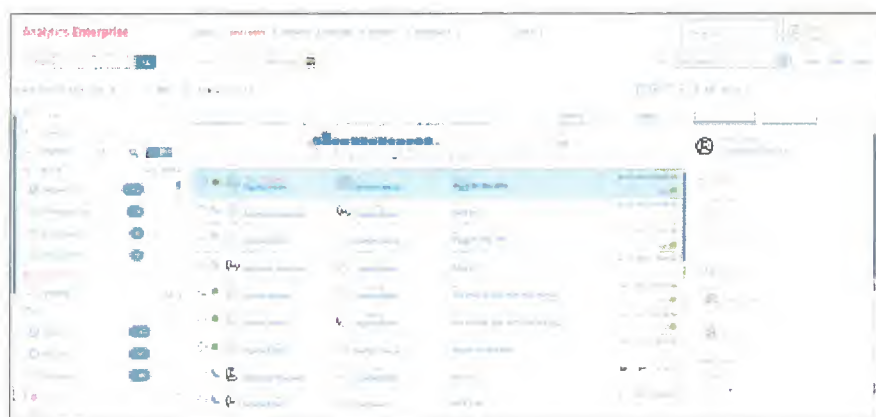
¹ Scalable to hundreds of millions of events in a multi-node, multi-server deployment

The following is an example of a case with over 95,000 events.



The Parties facet shows us that the data includes over 2,000 Parties, and that Tagobe Eddite has over 6,000 events. The Source facet shows that there are 37 Sources, and that there are over 2,000 WhatsApp events. This all appears without the user needing to click or search for anything.

When we select Tagobe Eddite in the Parties facet, the following outcome is displayed. The Source facet automatically updates to reflect the summarization of the current filtered data set: 1,400 Telegram events and 1,300 WhatsApp events (out of the over 2,000 that appeared before filtering for Tagobe's events only), in which Tagobe Eddite participated.



Cellebrite Inc.

7 Campus Drive
Suite 210
Parsippany New Jersey 07054
United States

Tel. +1 201 848 8552
Fax. +1 201 848 9982
Tax ID#: 22-3770059
DUNS: 033095568
CAGE: 4C9Q7
Company Website: <http://www.cellebrite.com>



Cellebrite

Digital intelligence
for a safer world

Quote

Quote# Q-43577-1
Date: Jun 08, 2018

Bill To

Alameda County Sheriff's Office
2901 Peralta Oaks Ct.
3rd FL
Oakland, California 94605
United States
Contact:
Phone:

Ship To

Alameda County Sheriff's Office
2901 Peralta Oaks Ct. 3rd FL
Oakland, CA 94605
United States

Contact:
Phone:

Customer ID	Good Through	Payment Terms	Currency	Sales Rep
SF-00040730	Jul 07, 2018	Net 30	USD	James Rowley

Product Code	Product Name	Qty	Start Date	End Date	Serial Number	Net Price/Unit	Net Price	Sales Tax %
B-AIS-02-050	UFED Premium Desktop including annual license and 50 actions	1				USD 100,000.00	USD 100,000.00	9.25
UFED Premium Desktop including annual license and 50 actions								
S-UFD-04-007	UFED Analytics Enterprise	1				USD 99,500.00	USD 99,500.00	0.00
UFED Analytics Enterprise								

SubTotal	USD 199,500.00
Shipping & Handling	USD 0.00
Sales Tax (4.64%)	USD 9,250.00
Total	USD 208,750.00

Comments:

Bundle of Total 140 Premium unlock actions and 10 user 500 searchable digital evidence units. Does not include server hardware for Analytics.

For further information please email James Rowley at james.rowley@cellebrite.com or call 760.783.1522

Terms and conditions:

- Payment terms: Net 30; 1.5% per month interest on late payment
- Shipping: FCA, Parsippany, NJ, USA : Limited Warranty: Hardware: 12 Months; Software: 60 days; Touch Screen: 30 days
- 12 months software support included in initial purchase. The next support period purchased begins immediately at the end of the 12 months, i.e., no gaps in support period are allowed.

Cellebrite has two different terms of sale.

Any purchase of unlocking services are governed by

<http://legal.cellebrite.com/CB-us-us/index.html>.

Any purchase of UFED Premium are governed by

<http://legal.cellebrite.com/home/usa-ufed-use-agreement-01292018.pdf>.

Any other purchases of products or services, including training, are governed by

<http://legal.cellebrite.com/us/index.html>.

In addition to these terms, software is licensed by Cellebrite in accordance with an end user license agreement available at

<http://legal.cellebrite.com/End-User-License-Agreement.htm>.

In the event of any dispute as to which terms apply, Cellebrite shall have the right to reasonably determine which terms apply to a given purchase order.

Quote Number: Q-43577-1

Prepared by James Rowley

Page 1 of 2

*SALES TAX DISCLAIMER: Cellebrite Inc. is required to collect Sales and Use Tax for purchases made from the following certain U.S. States. Orders are accepted with the understanding that such taxes and charges shall be added, as required by law. Where applicable, Cellebrite Inc. will charge sales tax unless you have a valid sales tax exemption certificate on file with Cellebrite Inc. Cellebrite Inc. will not refund tax amounts collected in the event a valid sales tax certificate is not provided. If you are exempt from sales tax, you must provide us with your sales tax exempt number and fax a copy of your sales tax exempt certificate to Cellebrite Inc.

Please include the following information on your PO for Cellebrite UFED purchase:

- Please include the ORIGINAL QUOTE NUMBER (For example - Q-XXXXX) on your PO
- CONTACT NAME & NUMBER of individual purchasing and bill to address
- E-MAIL ADDRESS of END USER for monthly software update as this is critical for future functionality